Spring 2020, Math 621: Week 9 Problem Set
Due: Friday, April 10th, 2020
Gröbner Bases

Warmup and Discussion problems. The problems below should be worked on in groups, but will not be submitted for credit. Only submit the homework problems at the end of this document. Try to read up through the start of the first discussion problem, and complete the warmup problems, prior to starting with your group. The content included covers enough material to complete the assigned problems, but if you are interested in further reading, I suggest Chapter 2 of *Ideals, Varieties, and Algorithms* by David Cox, John Little, and Donal O'Shea, or Chapter 15 of *Commutative Algebra with a View Toward Algebraic Geometry* by David Eisenbud.

As motivation for this week's content, consider the univariate polynomial ring $R = \Bbbk[x]$. We proved last semester that any ideal $I \subset R$ is principal, i.e., $I = \langle g(x) \rangle$ for some $g(x) \in I$. We even saw a convenient way to find $f(x)$: the Euclidean algorithm! As a refresher, if

$$I = \langle x^5 + 2x^4 - 2x^3 - x^2 + 3x - 1, x^4 + x^3 - 2x^2 + 3x - 1 \rangle,$$

then we repeatedly apply the division algorithm to obtain

$$\begin{aligned} x^5 + 2x^4 - 2x^3 - x^2 + 3x - 1 &= (x+1)(x^4 + x^3 - 2x^2 + 3x - 1) + (-x^3 - 2x^2 + x) \\ x^4 + x^3 - 2x^2 + 3x - 1 &= (x-1)(x^3 + 2x^2 - x) + (x^2 + 2x - 1) \\ x^3 + 2x^2 - x &= (-x)(x^2 + 2x - 1) + 0. \end{aligned}$$

At each step above, the remainder lies in I since the other terms in the equality all lie in I, ensuring $g(x) = x^2 + 2x - 1 \in I$. Moreover, by back-substituting, we see $g(x)$ divides both of the original generators of I. Together, these imply $I = \langle g(x) \rangle$.

(W1) Perform the Euclidean algorithm to find the (unique) monic principal generator of the ideal $I = \langle x^6 + x^4 + x^2, x^4 + x^3 + x \rangle \subset \mathbb{Q}[x]$.

Now, a lot of algorithmic questions involving polynomial ideals boil down to the following: given a polynomial $f(x)$ and an ideal I, is $f(x) \in I$? This is known as the *ideal membership problem*. For univariate polynomial rings, the above makes this easy: use the Euclicean algorithm to write $I = \langle g(x) \rangle$, then use the division algorithm to check if $g(x) \mid f(x)$. In particular, I contains precisely the polynomial multiples of $g(x)$.

For multivariate polynomial rings, the ideal membership problem becomes a lot more difficult. Not only are some ideals not principle (e.g., $\langle x, y \rangle \in \Bbbk[x, y]$), but even for those that are, the whole notion of "division algorithm" breaks down (e.g., there is no "natural" choice of remainder when dividing $x^2y + 3$ by $xy^2 + 5$).

The first hurdle to overcome: how do we choose the leading term of a multivariate polynomial? For instance, supposing $f = xy^9 + x^2z + xy^2 + 4$, which should the leading term be? In the end, this comes down to choosing a monomial ordering. Here are a few reasonable ways to do so.

- Lexicographic (lex) order: given two monomials $x^a, x^b \in \Bbbk[x_1, \ldots, x_k]$, we set $x^a \prec x^b$ if $a_1 < b_1$, or if $a_1 = b_1$ and $a_2 < b_2$, or if $a_1 = b_1$ and $a_2 = b_2$ and $a_3 < b_3$, and so forth. This is also known as "dictionary order", i.e., the standard way to alphabetize words.

  Under lex order: $f = x^2z + xy^9 + xy^2 + 4$, with terms written in descending order.

- Graded lexicographic (glex) order: we set $x^a \prec x^b$ if $a_1 + \cdots + a_k < b_1 + \cdots + b_k$, or if $a_1 + \cdots + a_k = b_1 + \cdots + b_k$ and x^a preceeds x^b under lex order. In particular, we compare total degrees of x^a and x^b, and then break ties using lex order.

  Under glex order: $f = xy^9 + x^2z + xy^2 + 4$, with terms written in descending order.

- Graded reverse lexicographic (grevlex) order: we set $x^a \prec x^b$ if $a_1+\cdots+a_k < b_1+\cdots+b_k$, or if $a_1+\cdots+a_k = b_1+\cdots+b_k$ and $a_k > b_k$, or if $a_k = b_k$ and $a_{k-1} > b_{k-1}$, and so on. Intuitively, after comparing total degrees, under glex smaller variables are more valuable, while under grevlex larger variables are undesirable.

  Under grevlex order: $f = xy^9 + xy^2 + x^2z + 4$, with terms written in descending order.

In general, a *term order* is a total ordering $\prec$ on the set of monomials in $R = \Bbbk[x_1, \ldots, x_k]$ (or, equivalently, on the elements of $\mathbb{Z}^k_{\geq 0}$) such that (i) if $x^a \prec x^b$, then $x^{a+c} \prec x^{b+c}$ for any $c \in \mathbb{Z}^k_{\geq 0}$; and (ii) every nonempty set of monomials has a least element under $\prec$. One can check that the 3 orderings defined above are indeed term orders. Also, each is defined by making a sequence of comparisons until a non-tie is reached; this is a common way to define term orders.

Now, once we choose a term order $\prec$, it at least gives us some (deterministic) way to perform polynomial long division. As an example, consider dividing

$$f = x^4y^2 + xy^2 - 2x \qquad \text{by} \qquad g_1 = xy^3 + x^2y - 2 \qquad \text{and} \qquad g_2 = x^2 - y$$

under the glex term order $\prec$. We first order the terms of each polynomial by $\prec$, as above. We then check the leading term of each g_i one by one until we find one that divides the leading term of f. Once we do, we scale it appropriately, and subtract to cancel the leading term of f. From there, we rinse and repeat until we obtain either 0 or a polynomial whose leading term is not divisible by the leading term of any g_i. The full division proceeds as follows.

$$\begin{array}{rll}
f: & x^4y^2 + xy^2 - 2x & \\
- & x^4y^2 - x^2y^3 & (= (x^2y^2)g_2) \\
\hline
 & x^2y^3 + xy^2 - 2x & \\
- & x^2y^3 + x^3y - 2x & (= (x)g_1) \\
\hline
 & -x^3y + xy^2 & \\
- & -x^3y + xy^2 & (= (-xy)g_2) \\
\hline
 & 0 &
\end{array}$$

At the end of the day, we obtain $f = (x)g_1 + (x^2y^2 - xy)g_2 + (0)$. If we instead use the lex term order, we obtain the following.

$$\begin{array}{rll}
f: & x^4y^2 + xy^2 - 2x & \\
- & x^4y^2 + x^3y^4 - 2x^2y & (= (x^2y)g_1) \\
\hline
 & -x^3y^4 + 2x^2y + xy^2 - 2x & \\
- & -x^3y^4 - x^2y^6 + 2xy^3 & (= (-xy^3)g_1) \\
\hline
 & x^2y^6 + 2x^2y - 2xy^3 + xy^2 - 2x & \\
- & x^2y^6 + xy^8 - 2y^5 & (= (y^5)g_1) \\
\hline
 & 2x^2y - xy^8 - 2xy^3 + xy^2 - 2x + 2y^5 & \\
- & 2x^2y + 2xy^3 - 4 & (= (2)g_1) \\
\hline
 & -xy^8 - 4xy^3 + xy^2 - 2x + 2y^5 + 4 &
\end{array}$$

Since xy^5 is not divisible by x^2y nor x^3 (the leading terms of g_1 and g_2 under lex order), we obtain

$$f = (x^2y - xy^3 + y^5 + 2)g_1 + (0)g_2 + (-xy^8 - 4xy^3 + xy^2 - 2x + 2y^5 + 4).$$

(W2) Perform polynomial long division with the above polynomials under glex order, but with g_2 listed before g_1. You should obtain a **different** remainder.

Remember that the goal is to determine if $f \in \langle g_1, g_2 \rangle$ by doing polynomial long division and checking the remainder. As the above examples demonstrate, this is not a reliable method

to use, as choosing a different term order (or even a different ordering of the g_i) can yield a different remainder. This is where Gröbner bases come in: if $I = \langle g_1, \ldots, g_r \rangle$ and the chosen generating set $g_1, \ldots, g_r$ is sufficiently nice, then the division algorithm can indeed be used to reliably determine membership in I.

Fix a term order $\prec$ on $R = \Bbbk[x_1, \ldots, x_k]$, and write $\mathrm{In}_\prec(f)$ for the leading term of f. A generating set $G = \{g_1, \ldots, g_r\}$ for I is a *Gröbner basis* with respect to $\prec$ if every $f \in I$, some $g_i \in G$ satisfies $\mathrm{In}_\prec(g_i) \mid \mathrm{In}_\prec(f)$. Notice that this is precisely what is needed to ensure division of any $f \in I$ by G is 0.

(D1) *Developing Buchberger's Algorithm.* In this problem, we will explore how to "grow" a given generating set into a Gröbner basis.

(a) Let $I = \langle g_1, g_2 \rangle \subset \Bbbk[x, y]$, where $g_1 = xy^3 + x^2y - 2$ and $g_2 = x^2 - y$. Verify that dividing $f = y^4 + xy^2 - 2x$ by $G = \{g_1, g_2\}$ has nonzero remainder (should be quick).

(b) Notice that $f \in I$ since

$$f = xg_1 - y^3 g_2 = x(xy^3 + x^2y - 2) - y^3(x^2 - y).$$

This highlights the main issue: the leading terms in this expression cancel and the new leading term is not divisible by the leading terms of g_1 and g_2. More generally, if $L = \mathrm{lcm}(\mathrm{In}_\prec(g), \mathrm{In}_\prec(h))$, the polynomial

$$S(g, h) = \frac{L}{\mathrm{In}_\prec(g)} g - \frac{L}{\mathrm{In}_\prec(h)} h$$

will (potentially) have this issue (we call this the *syzygy* or *S-polynomial* of g and h). Argue (briefly) that $S(g, h) \in I$ whenever $g, h \in I$.

(c) Buchberger's criterion tells us that syzygies are the only potential obstruction when assembling a Gröbner basis. Prove the forward direction.

Theorem ((Buchberger's Criterion)). *The set $G = \{g_1, \ldots, g_r\}$ is a Gröbner basis under $\prec$ if and only if every syzygy $S(g_i, g_j)$ has remainder 0 when divided by G.*

(d) Returning to our example, let's add $g_3 = S(g_1, g_2)$ to the list, so now $G = \{g_1, g_2, g_3\}$. Do any of the polynomials $S(g_i, g_j)$ yield a nonzero remainder when divided by G?

(e) (Reading only) It turns out that $\{g_1, g_2, g_3\}$ is indeed a Gröbner basis for I, and the last part above illustrates the idea behind *Buchberger's algorithm*: given a generating set $G = \{g_1, \ldots, g_r\}$, compute all syzygies $S(g_i, g_j)$ and divide each by G, then throw any nonzero remainders obtained into G. Continue in this manner until Buchberger's criterion is satisfied. This process can be quite long, but always terminates eventually 9we will see the key to proving this next week).

(f) Let $J = \langle x^3 - y^2, x^{10} - z^3 \rangle \subset \Bbbk[x, y, z]$. Use Buchberger's algorithm to find a Gröbner basis for J under the glex term order.

(g) Use your Gröbner basis to determine if $x^{11}z^3 - y^{14} \in J$.

It's worth noting that not all term orders are created equal, as some tend to yield **substantially** larger Gröbner bases than others. For instance, lex Gröbner bases tend to have a lot more elements than glex or grevlex Gröbner bases. In fact, most of the "popular" computer algebra implementations of Buchberger's algorithm default to grevlex order, since this tends to have particularly small Gröbner bases (though, strangely enough, no one has been able to prove this is the case; it has just been widely observed for "most" ideals).

Homework problems. You must submit *all* homework problems in order to receive full credit.

(H1) Use Buchberger's algorithm to obtain the reduced Gröbner basis for

$$I = \langle x^3 - wy^2, x^{10} - w^7 z^3 \rangle \subset \Bbbk[x, y, z, w]$$

under the grevlex term order.

(H2) Fix an $m \times k$ matrix M with row vectors $w_1, \ldots, w_m \in \mathbb{Z}^k_{\geq 0}$. Define an order $\prec_M$ on $R = \Bbbk[x_1, \ldots, x_k]$ so that $x^a \prec_M x^b$ whenever one of the following holds:

- if $a \cdot w_1 < b \cdot w_1$;
- if $a \cdot w_1 = b \cdot w_1$ but $a \cdot w_2 < b \cdot w_2$;
- if $a \cdot w_1 = b \cdot w_1$ and $a \cdot w_2 = b \cdot w_2$, but $a \cdot w_3 < b \cdot w_3$;

  $\vdots$
- if $a \cdot w_i = b \cdot w_i$ for all $i < m$, but $a \cdot w_m < b \cdot w_m$.

As an example, if $M = I$, then $\prec_M$ coincides with lex order. Determine for which M the order $\prec_M$ is a term order.

(H3) Fix a term order $\prec$ on $R = \Bbbk[x_1, \ldots, x_k]$, and fix nonzero polynomials $f, g \in R$. Prove that if $\gcd(\mathrm{In}_\prec(f), \mathrm{In}_\prec(g)) = 1$, then dividing $S(f, g)$ by f and g has remainder 0.

(H4) Determine whether each of the following statements is true or false. Prove your assertions.

(a) Under any term order $\prec$ on $\Bbbk[x_1, \ldots, x_k]$, for each variable x_i there are only finitely many monomials x^a such that $x^a \prec x_i$.

(b) Reverse lexicographic order, defined in the same manner as the grevlex term order but without the initial "total degree" comparison, is a term order.